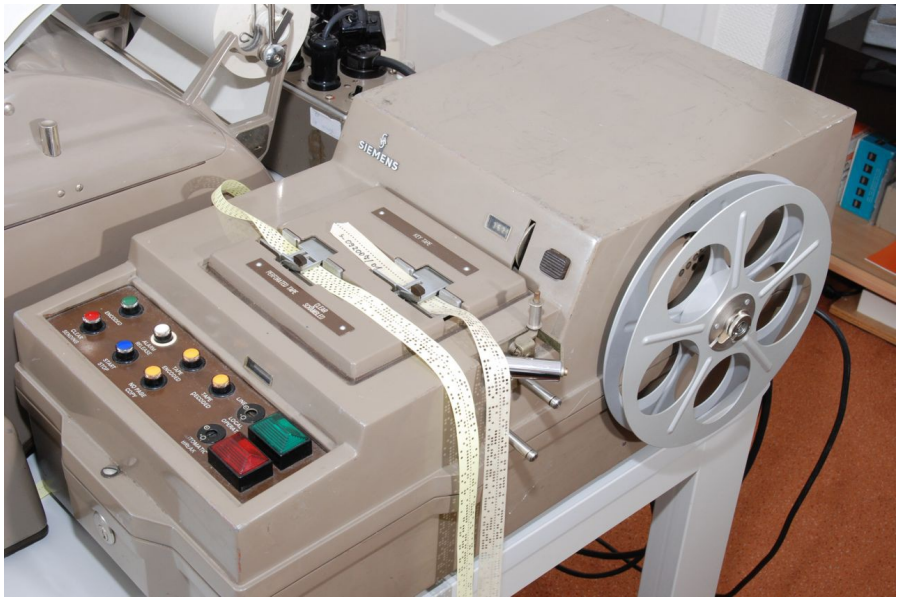
MANUAL FOR
SIEMENS T100Z / M190 CRYPTOSYSTEM
and
M190 Simulator



version 3.0, 2019.08.30

1. Introduction

Encryption techniques are very useful to prevent unauthorised organisations or people from accessing materiel that is of a classified or secret nature and the contents of which the originating organisation does not wish to be disclosed to others.

It is said that obtaining information from sources that wish to keep the information confidential, is the second oldest profession in the world, often assisted by the oldest profession.

One of the earliest instances known to the author was when a dictator wanted to keep his orders to high-ranking officials confidential. His solution was to shave the hair of a number of slaves and have their heads tattooed with the message, When the hair had regained the normal length, they were sent on their way. When they arrived, the official was informed that their hair was to be shaved off in order that the message could be read. In a way, this method could be compared to the one-time pads that we use today, as each slave could only be used once.

Until recently, systems designed to keep information confidential had a fatal flaw in that the secrecy could be penetrated if sufficient money and resources were thrown after it. The Enigma system that was used in the Second World War is a typical example of this.

To learn more about the accomplishments in this field, "The Code Book" by Jan Teuber is highly recommended reading. There is another book with an identical title written by Simon Singh. A visit to the virtual cryptography museum at www.cryptomuseum.com is highly recommended; https://en.wikipedia.org/wiki/One-time_pad is also a good site to visit.

Most of the hardware of the crypto system that is described in this manual was found in the Stevns Fortress which was one of the cornerstones in the defence of Denmark during the Cold War. Afterwards, the fortress was transformed into a Cold War museum.

The system to be described comprises two Siemens T100Z teleprinters and Siemens M190 Mixers. An identical system was used on the hotline between Washington and Moscow from 1980 to 1988 (see page 9 lower left corner). In its final years it was used as a backup for an IBM PC. As the number of M190 and equivalent mixers is very limited, the the M190 Simulator will also be described.

2. Common Transmission modes of the M/190 and Simulator

The M/190 has three transmission modes and two off-line routines.

- **Clear text:** This is the simplest transmission mode. It is simply sending and receiving a message on a standard teleprinter. It can be used to inform the operator which special actions need to be undertaken before the message can be sent.

- **Encrypted text**: In this mode the message is encrypted only within the transmission medium. In other words, the text sent and received will appear as plain text but an eavesdropper who taps into the communication line will only see the message in its encrypted form and hence he will not be able to read it. This mode requires the use of an identical key tape (which the unauthorized listener should not have access to...) at both stations

- **Scrambled mode**: This is the 'maximum security' mode as the operators at both ends will be unable to see the message. This mode should only be used when strictly necessary as it takes a lot of extra work and time which begs the question, why do we use this mode? It can be stated that the operators could be security risks because punched tapes could be lying around or even copies of received messages. This can be solved by having an off-line M/190 machine in the Operations Room where specially selected operators can punch the operation orders, encrypting them 'on the fly'. The encrypted tape can then be carried to the on-line M/190 in the Comms room, and be sent as if it were a normal message. However, a precaution must be taken. As the tape is encrypted, the operators at each end of the line must engage the NO HARD COPY button as the Carriage Return & Line Feed characters will also be encrypted with the result that most of the message will overprint as a block at the end of the line. Also, the answerback mechanism could be tripped, which would ruin the remainder of the message, as the key tape would loose its synchronisation.

- **Preparation**: This is an off-line routine that is used when an extremely sensitive message is to be prepared in a case where 'standard' operators are not allowed to see the message in clear text.

- **Decryption**: This is the reverse of Preparation. Sensitive and thus encrypted messages can be received normally and then carried to the Operations Room where they can be decrypted and an important issue concerning the creation of an encrypted tape must be

addressed here. Again : NO PAGE COPY must be activated

In production environments the normal procedure is to write the standard header in clear text followed by the Line Feed character, five Carriage Returns and one LTRS shift character.
The the encrypted part of the message starts at the first character AFTER the LTRS shift character.

For the simulator, there is a small difference. When positioning the key tape, it must be positioned at the LTRS character just in front of the message proper. This is because the simulator sends one character when starting up, just to synchronise everything.

In principle it is not important what kind of header is used as long as everyone agrees and people can find where the header ends.

In normal teleprinter traffic the standard method was to start the message tape with ZCZC and end with NNNN. It is generally acknowledged that these patterns were invented by Western Union staff and were used in their tape relay centres, as the patterns in the punched tape are easily recognisable.

3. Encryption Principles

The basic principle of encryption (and following decryption) is to change the message in accordance with a well-defined algorithm. This algorithm needs to be reversible, meaning that there must be a dependable way to retrieve the original text. If there isn't, then the meaning of the message will be lost.

The M190 Mixer combines the signals read from the reader for the message with the signals originating from the key tape reader and delivers the result to the transmission system. On arrival the receiving M190 reverses the encryption, and can print or punch the clear text.

In order to be able to reverse the action, identical key tapes must be used at both ends.

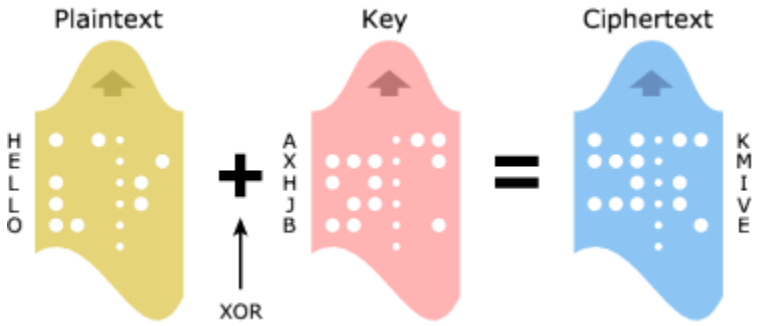
All encryption activities have a 'soft spot'. In the old days the message could often be decoded by sheer logic or by more or less politely asking the courier or an agent to divulge the key etc. Today, where encryption is unbreakable if you don't have the key, the 'soft spot' has shifted to logistics.

The best way to get key tapes to recipients is to deliver them personally by courier, so we can be sure that nosy foreign services cannot get to see the contents of the tape.
Just imagine the logistics burden and the overhead when a diplomatic service must distribute a weeks or a months worth of key tapes to the representatives in all the various countries. Some messages might even demand a special delivery.

Back to the mechanics.

A character as delivered by a teleprinter consists of 7 pulses: a start pulse, five data pulses corresponding to the five holes you can see in a punched tape and a stop pulse[1]. The start and stop pulses can be ignored in this discussion as they don't contain information : they are there for synchronisation only. The small holes in a tape are sprocket holes that are used to transport the tape through the tape reader but they also have a bonus function : they prevent the user from inserting a tape upside down, although they cannot prevent a tape from being placed in the reader upside down and backwards.

For every character read from the message tape, a character is read from the key tape.



The character 'H' on a punched tape appears like this **o-o.--** and an 'A' as **---.oo**
Now suppose that we want to send a letter H and the character on the key tape is an A.

What happens is that the two characters are added in a logical operation called 'Exclusive OR' (XOR). In plain language the two characters are compared one 'hole' at a time and a new character is constructed. This character will only contain holes in the positions where only one of the original tapes has a hole. So, if both tapes have a hole (or no hole) in the corresponding positions, there will be no hole in the output character.

1 The stop pulse normally has a length equal to 1,5 or 2 data pulses, so slightly different speedproblems can be cancelled out and the receiving system can synchronise itself with the sending system when a new character arrives.

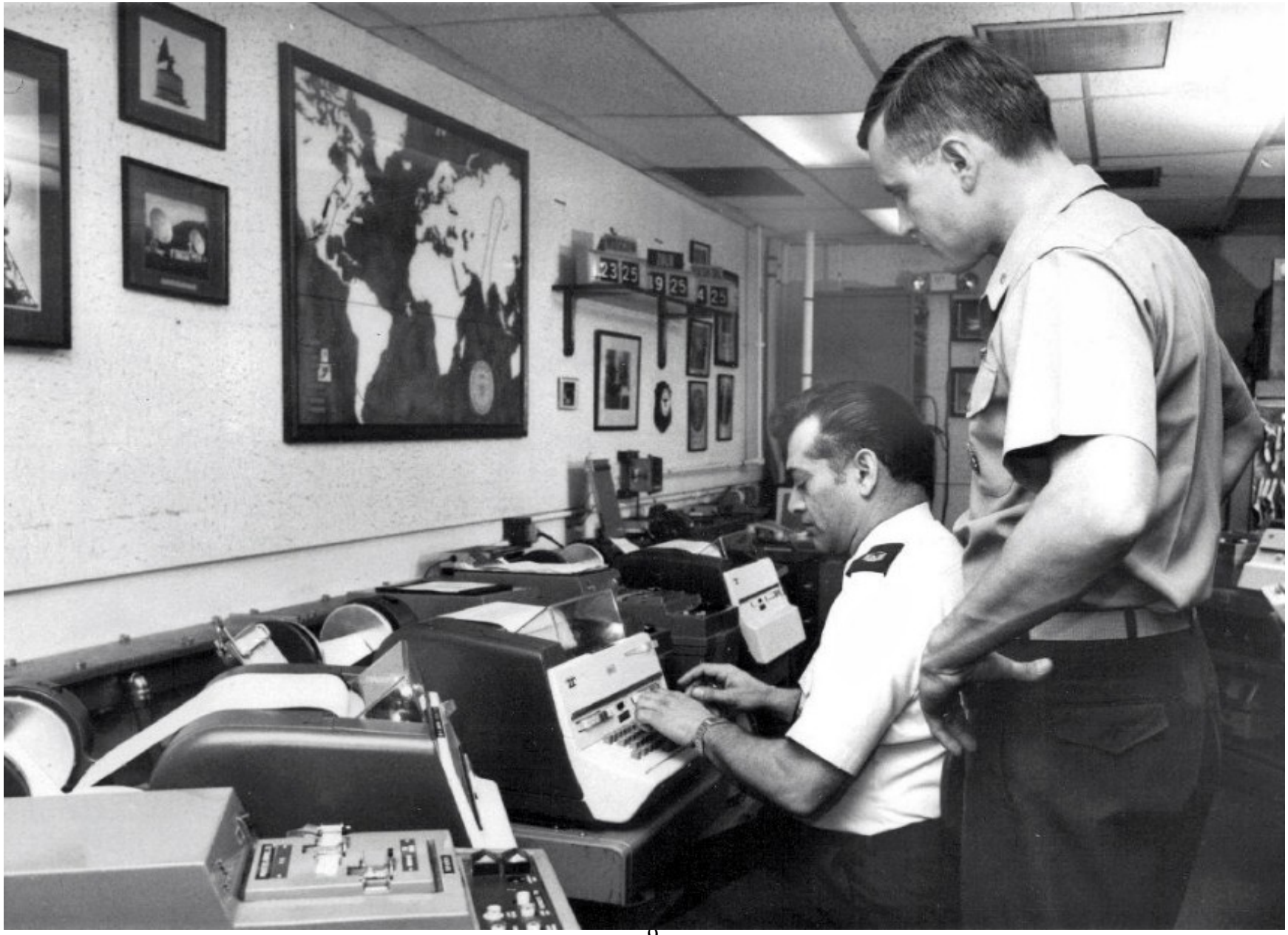
The resulting character is a K.

When receiving the reverse operation is carried out: 'XOR' the received K with the A from the key tape and the result will be a H.
In other words, the XOR is a reversible operation as long as you have the correct key tape.

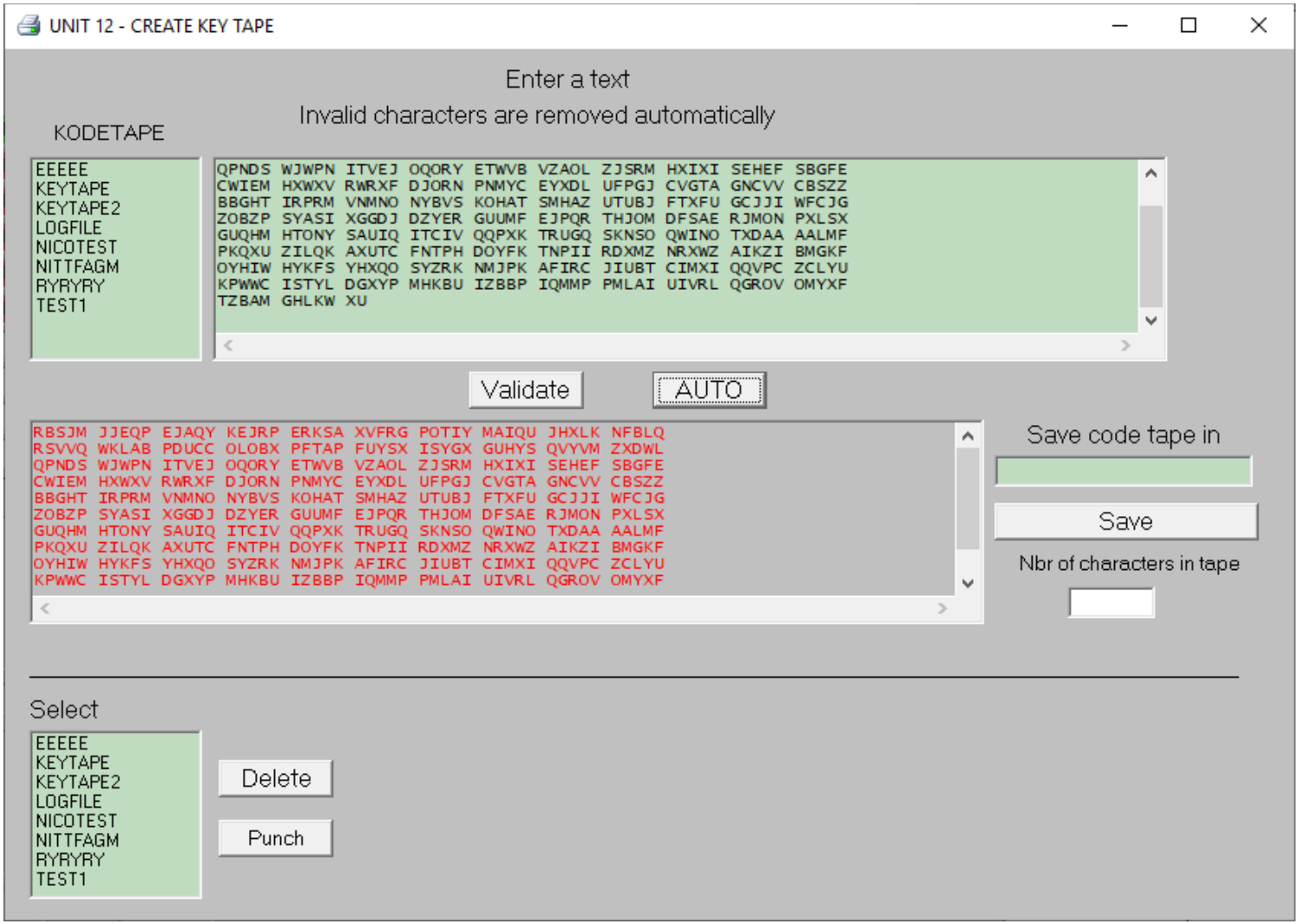
If a key tape with identical characters were to be used for encryption, it would be an easy job to reveal the message as it would only be necessary to do a maximum of 31 comparisons. The secret therefore is to make the key tape unpredictable and at least as long as the message to be sent.

Logic tells us that any character can be encrypted in 32 different ways (2^5), but some are better then others. Encrypting with a blank tape (having no holes apart from sprocket holes) is a bad idea because it will deliver the original message.

A more detailed explanation on the operations of a mixer can be found on http://cryptomuseum.com/crypto/siemens/m190/index.htm



4. The production of a key tape[2]



2 The spaces you can see in the box with the red letters are not used for encryption. They just make it easier to read.

A key tape should not be too short; it must be at least as long as the longest message ever expected to be sent.

In the Gentex Simulator the function **KEY TAPE** can be found.

A message text can be entered into the large green field. Any character can be used in the text but because of the limited character set of a teleprinter, any characters that are not used on teleprinters are to be removed.
This is done by pressing **VALIDATE**.

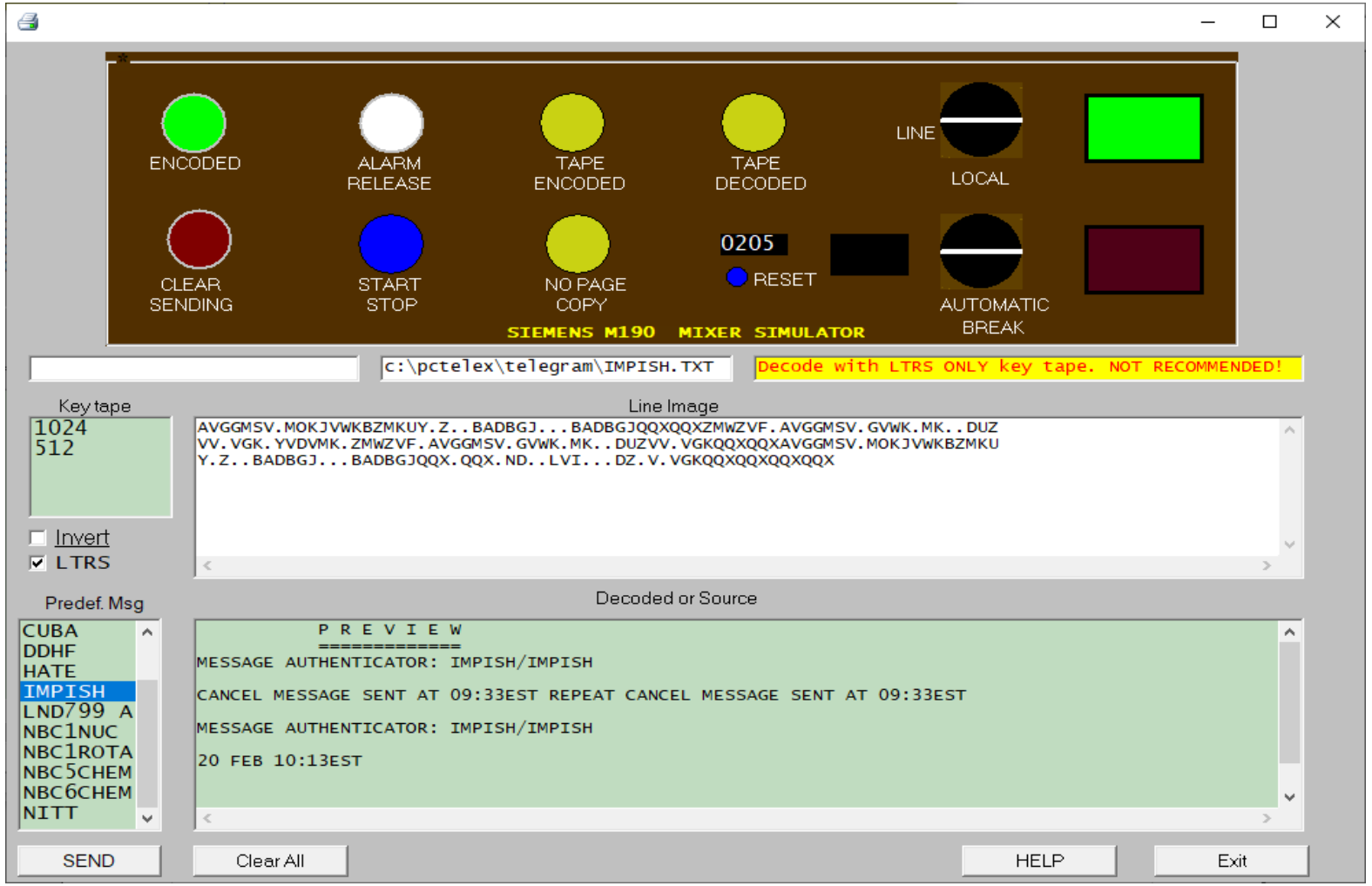
To simplify things and avoid predictable or repeated standard texts like “the quick brown fox jumps over the lazy dog” etc., a function **AUTO** has been implemented. This will generate a key tape with the specified length and although it is valid by definition, it must still be **VALIDATE**d.

After validating, the data will be saved as a text file and as an ITA2[3] image on the PC. This image is the electronic representation of the key tape and can be sent to the teleprinter tape punch. The image is also used by the M190 simulator, but more about that later.

The Simulator can be connected to the communication line so that the signals may be monitored be listening to the line signals[4].
In order to do that the correct key tape must be available.

3 ITA2 : character set for 5-channel teleprinters; vs. ASCII for 8-channel
4 It is recommended that the FJSKRTEST program is used for this purpose. It can also be used with just the M/190s and T100Z's, so no Simulator.

5. The Simulator



Not all installations will be able to find a genuine M190 and a T100Z let alone a complete set, so a M190 Simulator has been developed as a part of the Gentex Simulator so that 'full size' demonstrations can be accomplished, but this will probably take some preparation.

The screen is divided into three main parts :

- the operator panel, nearly identical to the M190;
- a part relating to what is being sent over the line;
- a part relating to the message that is intended to be sent or being received.

To the left of the **Line Image** box is a list of previously prepared key tapes. When a message is selected, it will be shown in the green box, preceded by two lines containing “P R E V I E W” resp “=========='. These lines will not be transmitted.

To the left of the **Decoded** box is a list of predefined messages. The message will be read one character at a time and will appear in the edit box underneath the Decoded box. If it has been specified that the message is to be encoded it will appear in the Line Image box.

LTRS is a switch which simulates a key tape consisting of LTRS only. This is very convenient when testing or doing a demonstration, but should not be used for “production” as you would need max 32 tests to find the encryption key.

INVERT is a switch which, when activated, inverts the signals sent to the communication medium. This switch had to be implemented as the physical M190 inverts the signals just before they are put on the transmission media, so you could risc clear text on the line.

AUTOMATIC BREAK is not used in the Simulator.

In Appendix A, a complete overview of the possible ways to operate a M190 Mixer may be found. Simulation of all functions in the Simulator have been embodied but for technical reasons a few of them have had to be adapted.

Sending :

- **ClearSending** This button indicates that you intend to send an unencrypted message. The input can come either from the keyboard or from a predefined message. When writing manually, the function will be deactivated if there is a

pause of 5 seconds. The transmission may be resumed by clicking **ClearSending** again.

- **Encoded** In order to send an encoded messag then the key tape to be used for the encryption must be specified. The message can either be written directly just as on a normal teleprinter or be previously prepared on a tape and sent via the Cleartext reader. The counter on the screen, between NO PAGE COPY and AUTOMATIC BREAK is the number of characters that have been read from the key tape. This should correspond with the number of characters read at the other side otherwise a disturbance of some kind has occurred and a part of the message will be garbled.
- **StartStop** This starts or stops the transmission but it is not relevant for manual transmission.
- **NO PAGE COPY** This button can be activated for security reasons when the operators are not permitted to see what is being written OR if an encrypted message is to be punched (printing encrypted messages on a teleprinter can be very annoying as it prints most of the message at the end of the line, and/or wastes a lot of paper because of false linefeeds)
- **Green lamp** System is safe (Encrypted operation);
- **Red lamp** System is in manual / unencrypted mode as in a normal teleprinter.

Receiving :

- **ClearSending** The default status is OFF. This enables reception of messages in clear-text form.
- **Encoded** If it is required to decode received messages 'on the fly' the required key tape to be used needs to be specified.
- **StartStop** This starts or stops the transmission but is only relevant for receiving encoded messages.
- **Automatic Break** This feature is not present in the Simulator. On a real M190, the function is used to interrupt the message transmission. This could be relevant when a recipient runs out of paper or has technical problems, or a FLASH

message is to be transmitted.

- **Counter** The counter shows how many characters have been read from the key tape so that the operator can check with his counterpart that no characters have been lost 'en route'.

- **Green lamp** This indicates that the system is safe (Encrypted operation).
- **Red lamp** System is in manual / unencrypted mode as with a normal teleprinter.

Other functions:

- **TapeEncoded** This button is used when it is necessary to prepare a message with input from the keyboard or a predefined message. For obvious reasons the key tape to be used for the encoding needs to be specified.

- **TapeDecoded** This is used for decoding a received encoded message.

- **AlarmRelease** Any error will generate an alarm sound and the lamp inside the button will light up. The alarm can be cancelled by pressing this button.

- **Line/Local** When coded messages are to be prepared, it is recommended to take the system off-line. This is not relevant in the Simulator, as the PC has no attached tape punch, so we must use a teletype for this purpose. The switch must be used when decoding received encrypted messages.

- **Counter** The counter shows how many characters have been read from the key tape to enable checking with the other end of the circuit that the correct number of characters has been received.

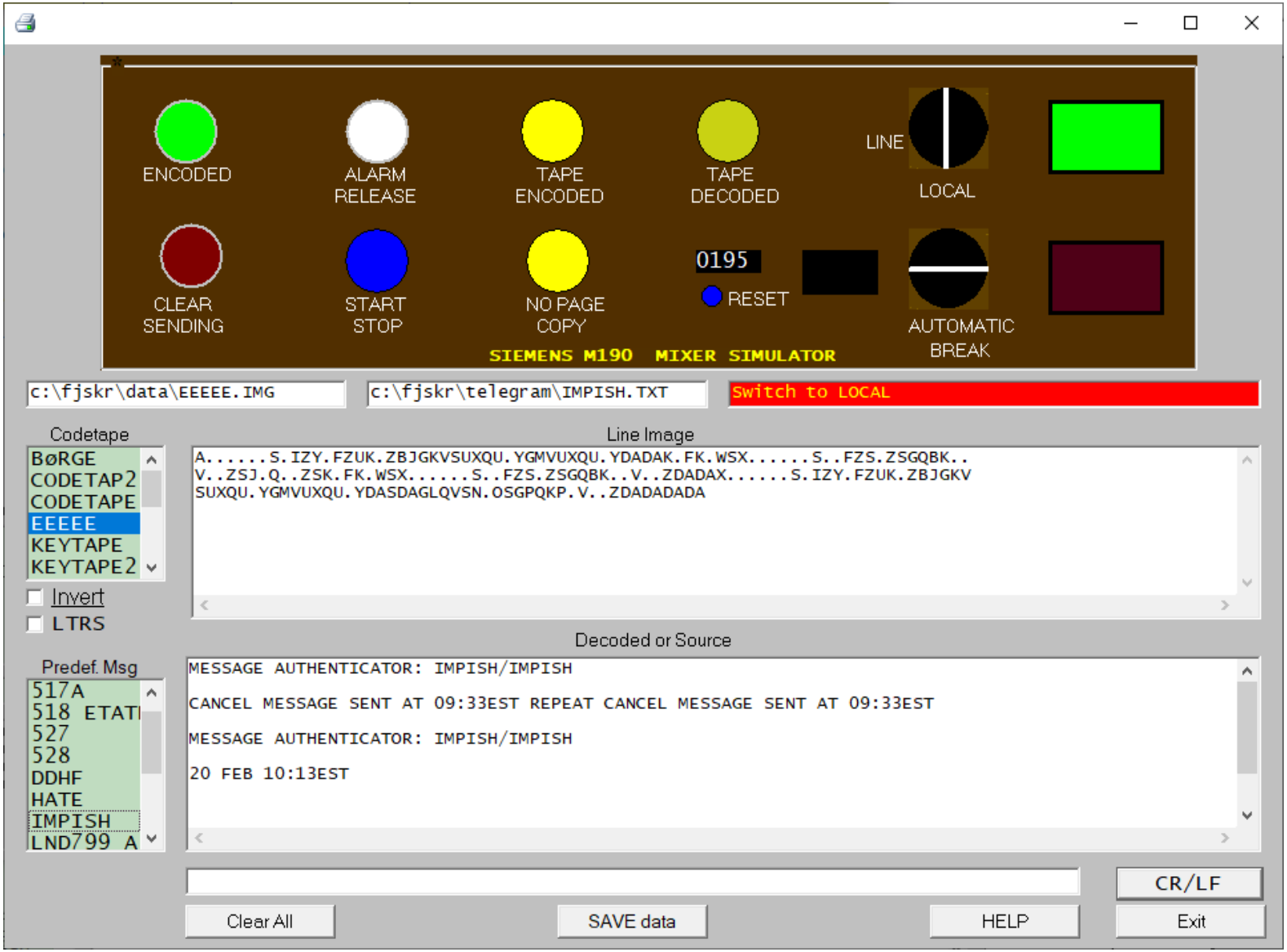
- **Advance** There is a black button to the right of the Counter which advances the counter by one and steps the key tape one position forward. It can be used when the key tapes are out of step so the operator with the lowest number in the counter can step up to the value shown to the other operator. By doing this it is possible to resume a transmission after synchronization of the key tapes.

The system will normally be in '**Receive clear text**' mode, however, this doesn't mean that the received text will be readable.

If a classified message is to be received as 'eyes only' for the unit commander, then the operator must activate the tape punch and the **NO PAGE COPY** button. The encoded tape will then be carried to the OpCenter where a stand-alone encryption set is located[5].
The encoded tape will be put into the **CLEAR TEXT** reader and the proper key tape in the **KEY TAPE** reader and on pressing the **TAPE DECODED** button, the clear text message will be printed.

The screen shot on the next page shows the result of **TAPE ENCODED**, meaning that a paper tape containing the encoded version of a cleartext message has been prepared.

5 An alternative is to switch the M190 to off-line / local


ENCODED
ALARM RELEASE
TAPE ENCODED
TAPE DECODED
LINE
LOCAL
CLEAR SENDING
START STOP
NO PAGE COPY
0195
RESET
AUTOMATIC BREAK
SIEMENS M190 MIXER SIMULATOR
c:\fjskr\data\EEEEE.IMG
c:\fjskr\telegram\IMPISH.TXT
Switch to LOCAL
Codetape
BøRGE
CODETAP2
CODETAPE
EEEEE
KEYTAPE
KEYTAPE2
Invert
LTRS
Line Image
A.....S.IZY.FZUK.ZBJGKVSUXQU.YGMVUXQU.YDADAK.FK.WSX.....S..FZS.ZSGQBK..
V..ZSJ.Q..ZSK.FK.WSX.....S..FZS.ZSGQBK..V..ZDADAX.....S.IZY.FZUK.ZBJGKV
SUXQU.YGMVUXQU.YDASDAGLQVSN.OSGPQKP.V..ZDADADADA
Decoded or Source
MESSAGE AUTHENTICATOR: IMPISH/IMPISH
CANCEL MESSAGE SENT AT 09:33EST REPEAT CANCEL MESSAGE SENT AT 09:33EST
MESSAGE AUTHENTICATOR: IMPISH/IMPISH
20 FEB 10:13EST
Predef. Msg
517A
518 ETAT
527
528
DDHF
HATE
IMPISH
LND799 A
CR/LF
Clear All
SAVE data
HELP
Exit

The first line below the operator panel contains three fields: the name of the key tape, the name of the file to be transmitted, and a field for error messages. These messages will be cleared when **ALARM RELEASE** is pressed.

It will be noticed that **TAPE ENCODED** has changed its colour. The Green lamp is lit (albeit not very clearly) to indicate that the system is working in Encrypted mode. **NO PAGE COPY** is also activated, as we would otherwise print the encoded message.

As soon as the message has been sent the selection bar in ”Predef. Msg” will have changed to a dotted envelope in order to avoid a retransmission.
The counter shows the number 195 which will probably be a bit more than the number of characters in the message itself. This is because the number 195 reflects the number of characters used from the key tape and not necessarily the number of characters in the message.

The encoded message will appear to contain a lot of periods. This is not really the case because a period represents a non-printable character like Carriage Return (CR) and Line Feed(LF) etc.

<u>The overriding priority in all encryption systems is to keep the key tape(s) secure.</u>

6. Operation of the mixer

6.1 Basic functions.

Most of the information in this sub-chapter is taken from Chapter 1 in ”Kryptoforsats M/190 Beskrivelse” issued by the Danish Telegraph Regiment.

The Mixer has the following modes of operation as follows:

- send tapes unencrypted
- send tapes encrypted
- write manually unencrypted
- write manually encrypted
- local writing/punching/unencryption

Refer to Appendix A.

The standard mode is clear text communication.
Transmission of prepared messages is initiated by pressing START/STOP.
All code tapes could be transmitted in this way but that would be a violation of the first principle in encryption: i.e. To keep the key tapes safe, secure and uncompromised.

Unencrypted communication is accomplished by pressing CLEAR SENDING during which time the red lamp at the right hand side of the unit will be lit to show that the communication is insecure.

To ensure that the operator is aware that the transmission is insecure, the lamp will be interrupted after 4-7 seconds of 'silence' and ALARM RELEASE will be lit up. In order to continue with the transmission, the alarm must be cleared and CLEAR SENDING must be reactivated.

The unit has a number of special functions:

- NO PAGE COPY ensures that the received messages are not printed on the teleprinter, so it must be remembered to enable the tape punch. The purpose of this is to ensure that unauthorised persons do not see the message whether encrypted or not. The tape is then delivered to the Operations officer for local decryption and printing[6]
- LINE / LOCAL OPERATION is normally in LINE mode which means that everything typed is transmitted onto the communication line. LOCAL mode may be used to prepare tapes or when it is necessary to change the paper etc., or when it is required to decrypt and print a message or copy a key tape.

The printer and the mixer are not accessible from the outside when LOCAL mode is active.

When AUTOMATIC BREAK is active the transmission of data will be interrupted when something is received from the other station. This should be avoided as the current transmission will need to be repeated probably with a different key tape.
This function is not supported in the Simulator.

6 which of course requires that he also has the relevant key tape !

6.2 Summary of the most frequently used functions

Manual Transmission

- Press CLEAR SENDING
- RED LAMP will be lit.
- Begin typing the message.
- If typing is paused for 4-6 seconds the CLEAR SENDING lamp will be extinguished.
- Press CLEAR SENDING to resume transmission.

Transmission of a prepared tape with CLEAR TEXT

- Insert tape in SCRAMBLED TAPE reader
- Press CLEAR SENDING
- Press START/STOP
- Keep CLEAR SENDING depressed while transmitting

Manual transmission of encrypted message

- Press ENCODED
- Ensure that ENCODED mode is active on receiving M/190.
- GREEN LAMP is lit
- Begin typing the message
- (If ENCODED mode is not active, then the message will be printed in encoded form)

Transmission of a prepared tape in CLEAR TEXT, but with ENCODED data on transmission media

- Press ENCODED
- Ensure that ENCODED is active on receiving M/190.
- GREEN LAMP is lit
- Press START/STOP

Preparing an encoded tape off-line

- Turn the switch LINE/LOCAL 1/4 turn clockwise, so the groove points at LOCAL
- Insert Key tape
- Press ENCODED
- Activate paper tape punch
- Start typing, OR
- Insert pre-punched message tape in CLEAR TEXT reader, and press START/STOP

7. Considerations regarding listening in

In order to listen in on an encrypted line a copy of the key tape will be needed and the start positions must be identical.
An appropriate demonstration would be to shift the key tape one position[7].

The problem with listening in is that what is received from the line is utterly incomprehensible; this is because of the XOR operation that has been done by the originator.

It is therefore quite possible that what is seen on the line is a mixture of shift and other characters and at some point one of them will trip the answer-back mechanism into operation.

A special filter prevents this from happening by replacing all shift and other non printing characters with a full stop. Figures and special characters will be replaced by their unshifted values; e.g. a '-' will be showsn as an 'A'.

Another way to listen in on the encrypted line is to connect a PC that is running the FJSKRTEST program. This will make the listening-in operation independent from the Simulator program.

7 There is a special function in the Simulator to show the effect

Appendix A

	Mode		Input	Button(s)	Line / Local	Cleartext-reader	Keytape-reader	Print	Tapepunch produces	Lamp lit
1	Transmit	Cleartext	Keyboard	Clear	Line	---	---	Cleartext	Cleartext	
2	Transmit	Cleartext	Cleartextreader	Clear Start	Line	Cleartext	---	Cleartext	Cleartext	
3	Receive	Cleartext		---	Line	---	---	Cleartext	Cleartext	
4	Transmit	Encrypted	Keyboard	Encoded	Line	---	Keytape	Cleartext	Cleartext	
5	Transmit	Encrypted	Cleartextreader	Encoded Start	Line	Cleartext	Keytape	Cleartext	Cleartext	
6	Receive	Encrypted		Encoded	Line	---	Keytape	Cleartext	Cleartext	
7	Prepare	Encrypted tape	Keyboard	Tape Encoded	Local	---	Keytape	---	Encrypted text	
8	Prepare	Encrypted tape	Cleartextreader	Tape Encoded Start	Local	Cleartext	Keytape	---	Encrypted text	
9	Transmit	Encrypted tape	Cleartextreader	Clear No Page Copy Start	Line	Encrypted tape	---	---	Encrypted text	
10	Receive	Encrypted tape		No Page Copy Clear	Line	---	---	---	Encrypted text	
11	Decode	Encrypted tape		Tape Decoded	Local	Encrypted tape	Keytape	Cleartext	Cleartext	

'Encrypted tape' is the tape containing the message AFTER it has been encoded by means of the KEYTAPE
'Cleartext tape' is the tape containing an unencrypted message

Appendix B

	Betriebsart		Gedrückte Leuchttaste	Drehtaste mit/ohne Ltg.	Klar LS	Schlüssel LS	Abdruck	Locher Locht	Bemerkung
Klarbetrieb	Sendung	Von Tastatur	Dauernd Klar (rot)	Mit Ltg.	-	-	Klar-Text	Klar-Text	
Klarbetrieb	Sendung	Vom Klar-Lochstreifen leser	Klar (rot) Start (Blau)	Mit Ltg	Klar-Text	-	Klar-Text	Klar-Text	
Klarbetrieb	Empfang		---	Mit Ltg	-	-	Klar-Text	Klar-Text	
Verschlüsselter Betrieb	Sendung	Von Tastatur	Verschlüsseln (Grün)	Mit Ltg	-	Schlüssel	Klar-Text	Klar-Text	
Verschlüsselter Betrieb	Sendung	Vom Klar-Lochstreifen leser	Verschlüsseln (Grün) Start (Blau)	Mit Ltg	Klar-Text	Schlüssel	Klar-Text	Klar-Text	
Verschlüsselter Betrieb	Empfang		Verschlüsseln (Grün)	Mit Ltg	-	Schlüssel	Klar-Text	Klar-Text	
Betrieb mit verschlüsseltem Lochstreifen	Herstellung (lokal) mit Tastatur	Von Tastatur	Verschlüsseln mit Lochstreifen (Gelb)	Ohne Ltg. Oder T56	-	Schlüssel	-	Klar-Text	
Betrieb mit verschlüsseltem Lochstreifen	Herstellung (lokal) mit Lochstreifen sender	Lochstreifen sender	Verschlüsseln mit Lochstreifen (Gelb) Start (Blau)	Ohne Ltg. Oder T56	Klar-Text	Schlüssel	-	Klar-Text	
Betrieb mit verschlüsseltem Lochstreifen	Sendung	Vom Klar-Lochstreifen leser	Dauernd Klar (Rot) Ohne Mitlesen (Gelb) Start (Blau)	Mit Ltg	Verschlüsselter Text	-	-	Verschlüsselter Text	
Betrieb mit verschlüsseltem Lochstreifen	Empfang		Ohne Mitlesen (Gelb)	Mit Ltg	-	-	-	Verschlüsselter Text	
Betrieb mit verschlüsseltem Lochstreifen	Entschlüsselung (Lokal)		Entschlüsseln mit Lochstreifen (Gelb)	Ohne Ltg. Oder T56	Verschlüsselter Text	Schlüssel	Klar-Text	Klar-Text	

Pause max. 4 – 7 Sek nur bei mit Ltg
Taste Klarsendung festhalten nur bei Ltg
Start /Stop startet stopp den Klarleser